CLAIMS

What is claimed is:

1. An ephemeral-output-only browser.

2. A system for protecting content distributed through a network comprising:

a client computer operable for connecting to the network and for executing a client program that limits user control over the content distributed through the network; and

a server computer operable for connecting to the network and for executing a security program for securing the content distributed through the network.

3. The system of claim 2, wherein the client program is an ephemeral-output-only web browser.

4. The system of claim 2, wherein the client program is an add-in security module for executing as part of a standard web browser and wherein user control over reproduction of the content, in at least one form, is limited.

5. The system of claim 2, wherein the client program executes as a separate window in a standard web browser and wherein user control over reproduction of the content, in at least one form, is limited.

6. The system of claim 2, wherein the security program distributes the content to the client computer only when the client computer is executing the client program, in at least one form, is limited.

7. The system of claim 2, wherein the security program secures the content using a common security model.

8. The system of claim 2, wherein the security program secures a portion of the content using an individual security model.

9. The system of claim 2, wherein the client program limits user control over the content through a technique chosen from the group consisting of:

message monitoring, clipboard flushing, function disabling, source code encryption, content localization, secure document packaging, cache encryption, and device content monitoring,

and wherein user control over reproduction of the content in any non-ephemeral output manner is prevented.

10. A method of enabling a provider to protect content distributed on a network comprising:

acquiring a server security program;

executing the server security program on a server computer connected to the network; and

distributing the content only to a client computer executing a limited-user client program which limits reproduction of the content in at least one form.

11. The method of claim 10, further comprising:

acquiring a plurality of copies of the limited-user client program; and

downloading one of the plurality of copies to the client computer.

12. The method of claim 10, wherein distributing the content comprises:

obtaining a promise of compensation from a user of the client computer.

13. The method of claim 12, wherein the compensation is a one-time fee.

14. The method of claim 12, wherein the compensation is a subscription fee.

15. The method of claim 12, wherein the compensation is a per-session fee.

16. The method of claim 12, wherein the compensation is a per-access fee.

17. The method of claim 12, wherein the limited-use client program disables a certain user function and the compensation comprises a fee for re-enabling the certain user function.

18. The method of claim 17, wherein the certain user function modifies the content.

19. The method of claim 17, wherein the certain user function copies the content to a different medium.

20. A method of receiving compensation for a security system for protecting content distributed on a network comprising:

selling a server security program to a content provider; and

selling a plurality of copies for a limited-use client program to the content provider for licensing to users wishing to access the content.

21. The method of claim 20, wherein the compensation is received at least from one of (a) when the server security program is executed by the content provider and (b) when the content provider licenses one of the plurality of copies.

22. The method of claim 20, wherein the server security program distributes the content to a client system if the client system has a limited-use client program and wherein the limited-use client program limits reproduction of the content in at least one way.

23. The method of claim 20, wherein the compensation is based on advertising revenue obtained by the content provider based on advertising displayed in connection with a user accessing content protected by the security system.

24. A method for controlling access to information presented by a web browser comprising:

presenting content within a browser window of the web browser; and

disabling a disallowed user function when the content is within the browser window.

25. The method of claim 24, wherein disabling the disallowed user function comprises:

intercepting a message posted to the browser window; and

hiding the content if the browser is not a foreground application.

26. The method of claim 24, wherein disabling the disallowed user function comprises:

clearing a commonly shared inter-application memory when the inter-application memory is accessed.

27. The method of claim 24 wherein disabling the disallowed user function comprises:

hiding a user menu selection corresponding to the disallowed user function.

28. The method of claim 24, wherein disabling the disallowed user function comprises:

intercepting a keyboard message; and

discarding the keyboard message if it corresponds to the disallowed user function.

29. The method of claim 24, wherein disabling the disallowed user function comprises:

monitoring a context for a device; and

discarding a user action directed to the device when the context matches the content.

30. The method of clam 24, wherein the disallowed user function is one of a plurality of default disallowed user functions and further comprising:

leaving active one of the plurality of default disallowed user functions.

31. The method of 30, further comprising providing information with the content that determines the one of the plurality of default disallowed user functions to be left active.

32. The method of claim 24 wherein the disallowed user function is selected from the group consisting of print, page setup, save, save as, view source, save picture as, set as wallpaper, copy, screen capture, screen print, cut.

33. The method of claim 24 further comprising managing authentication of a web client.

34. The method of claim 24 further comprising processing a request from a web client for encrypted content.

35. The method of claim 24 further comprising creating a unique identifier for a web client.

36. The method of claim 24 further comprising encrypting the content with a key based on the unique identifier for the web client.

37. The method of claim 24 wherein the content comprises user perceivable information in a hyper-text markup language (HTML) format.

38. The method of claim 24 wherein the content comprises user perceivable streaming information.

39. The method of claim 24 wherein the content comprises at least one of video information and audio information.

40. The method of claim 24 wherein the disallowed user function comprises a user function which, when allowed, provides for non-ephemeral reproduction of the content.

41. The method of claim 24 wherein the content comprises user perceivable information in a scripting language format.

42. The method of claim 24 wherein the content comprises user perceivable information in a common gateway interface (CGI) language format.

43. The method of claim 24 wherein the content comprises user perceivable information in a JAVA language format.

44. A computer-readable medium having stored thereon computer executable instructions to cause a client digital processing system and a server digital processing system to perform a method comprising:

transmitting content from the server digital processing system to the client digital processing system over a network;

presenting the content within a browser window on the client digital processing system; and

disabling a disallowed user function when the content is within the browser window wherein the disallowed user function comprises a user function which, when allowed, provides for non-ephemeral reproduction of the content.

45. The computer-readable medium of claim 44 wherein disabling the disallowed user function comprises:

intercepting a message posted to the browser window; and

hiding the content if the browser is not a foreground application.

46. The computer readable medium of claim 44 wherein disabling the disallowed user function comprises:

clearing a commonly shared inter-application memory if the inter-application memory is accessed.

47. The computer readable medium of claim 44 wherein disabling the disallowed user function comprises:

hiding a user menu selection corresponding to the disallowed user function.

48. The computer readable medium of claim 44, wherein disabling the disallowed user function comprises:

intercepting a keyboard message; and

discarding the keyboard message if it corresponds to the disallowed user function.

49. The computer readable medium of claim 44, wherein disabling the disallowed user function comprises:

monitoring a context for a device; and

discarding a user action directed to the device when the context matches the content.

50. The computer readable medium of claim 44 further comprising instructions to cause the server digital processing system to manage the authentication of the client digital processing system.

51. The computer readable medium of claim 44 further comprising instructions to cause the server digital processing system to process a request from of the client digital processing system for encrypted content.

52. The computer readable medium of claim 44 further comprising instructions to cause the client digital processing system to create a unique identifier for the client digital processing system.

53. The computer readable medium of claim 52 further comprising instructions to cause the client digital processing system to encrypt the content with a key based on the unique identifier.

54. The computer readable medium of claim 44 wherein the pre-determined function is selected from the group consisting of print, page setup, save, save as, view source, save picture as, set as wallpaper, copy, screen capture, screen print, cut.

55. A client digital processing system for controlling access to content presented by a web browser, the client digital processing system comprising:

a processor;

a network interface logically coupled to the processor to receive the content;

a browser logically coupled to the network interface to present the content within a browser window; and

a security module logically coupled to the browser to disable disallowed user functions when the content is in the browser window wherein the disallowed user function comprises a user function which, when allowed, provides for non-ephemeral reproduction of the content.

56. The client digital processing system of claim 55, wherein the security module comprises:

a message monitor to intercept a message posted to the browser window; and

a browser controller logically coupled to the message monitor to hide the content if the browser is not a foreground application.

57. The client digital processing system of claim 55, wherein the security module comprises a browser controller that clears a commonly shared inter-application memory when the inter-application memory is accessed.

58. The client digital processing system of claim 55, wherein the security module comprises a browser controller that encrypts the content.

SUB C2

59. A server digital processing system for controlling access to content distributed to a client digital processing system, the server digital processing system comprising:

a processor;

a network interface logically coupled to the processor to receive a request for the content from the client digital processing system;

a server module logically coupled to the network interface to distribute the content to the client digital processing system in response to the request; and

a security module logically coupled to the server module to determine if the request is from a client digital processing system executing a limited-use client program which prevents at least one form of non-ephemeral reproduction.

60. The server digital processing system of claim 59, wherein the security module is further operable to:

create a secure document object containing the content if the content is protected under an individual security model; and

pass the secure document object to the server module for distribution in response to the request.

61. The server digital processing system of claim 59, wherein the security module is further operable to:

encrypt the content if the content is protected under a common security model; and

pass the encrypted content to the server module for distribution in response to the request.

62. A computer-readable medium having stored thereon computer executable instructions to cause a client digital processing system to perform a method comprising:

receiving protected content from a server digital processing system;

presenting the protected content within a browser window; and

disabling disallowed user functions when the protected content is in the browser window wherein the disallowed user function comprises a user function which, when allowed, provides for non-ephemeral reproduction of the content.

63. The computer-readable medium of claim 62 further comprising:

intercepting a message posted to the browser window; and

hiding the protected content if the browser is not a foreground application.

64. A computer readable medium of claim 62 wherein the disallowed user function is enabled when content in the browser window is not designated to be protected such that non-ephemeral reproduction of such content is allowed.

65. A computer-readable medium having stored thereon computer executable instructions to cause a server digital processing system to perform a method comprising:

receiving a request for protected content from a client digital processing system;

determining if the request is from a client digital processing system executing a limited-use client program; and

distributing the protected content to the client digital processing system in response to the request only if the client digital processing system is executing the limited-use client program, wherein the limited-use client program prevents at least one form of non-ephemeral reproduction of the protected content.

66. The computer-readable medium of claim 65, further comprising:

creating a secure document object containing the protected content if the content is protected under an individual security model; and

passing the secure document object to the server module for distribution in response to the request.

67. The computer-readable medium of claim 65, further comprising:

encrypting the protected content if the content is protected under a common security model; and

passing the encrypted content to the server module for distribution in response to the request.

68. A computer readable medium of claim 65 wherein the limited-use client program disables a disallowed user function that comprises a user function which, when allowed, provides for non-ephemeral reproduction of the content.

69. A computer readable medium of claim 68 wherein the disallowed user function is enabled when content is not designated to be protected such that non-ephemeral reproduction of such content is allowed.

70. A computer readable medium of claim 69 wherein non-ephemeral reproduction of the protected content is allowed after a transaction between the client digital processing system and the server digital processing system.

71. A computer readable medium of claim 70 wherein the transaction comprises at least one of a compensation to a provider of the protected content or an exchange of identification of the client digital processing system.

72. A computer readable medium having stored thereon a secure document package data structure comprising:

a document package header field containing data representing a description for the secure document package;

a delivery object field containing data representing executable code to manage the secure document package described by the document package header field; and

a document field containing data representing content contained in the secure document package described by the document package header field.

73. The computer readable medium of claim 72, wherein the document package header field comprises:

a package identifier field containing data representing an identifier for the secure document package.

74. The computer readable medium of claim 72, wherein the document field comprises:

a document identifier field containing data representing an identifier for the content.

75. A computer data signal embodied in a carrier wave and encoding a data structure containing protected content comprising:

a document package header field containing data representing a description for the secure document package;

a delivery object field containing data representing executable code to manage the secure document package described by the document package header field; and

a document field containing data representing content contained in the secure document package described by the document package header field.

76. The computer readable medium of claim 75, wherein the document package header field comprises:

a package identifier field containing data representing an identifier for the secure document package.

77. The computer readable medium of claim 75, wherein the document field comprises:

a document identifier field containing data representing an identifier for the content.

sub C10

78. A system for controlling reproduction of content on a client computer comprising:

means for receiving content to be protected; and

means for displaying the protected content on the client computer while preventing at least one form of reproduction of the content.

H1 Cont'd

79. The system of claim 78, wherein the means for displaying comprises:

means for disabling user functions that reproduce the content.

80. The system of claim 79, wherein the means for displaying further comprises:
means for enabling disabled user functions under pre-determined conditions.

81. A system for controlling reproduction of content stored on a server computer comprising:
means for protecting content stored on the server;
means for receiving a request for the protected content; and
means for determining if the request is from a requestor that limits reproduction of protected content.

82. The system of claim 81, wherein the means for protecting comprises:
means for creating a secure document object containing the content.

83. The system of claim 81, wherein the means for protecting comprises:
means for encrypting the content.